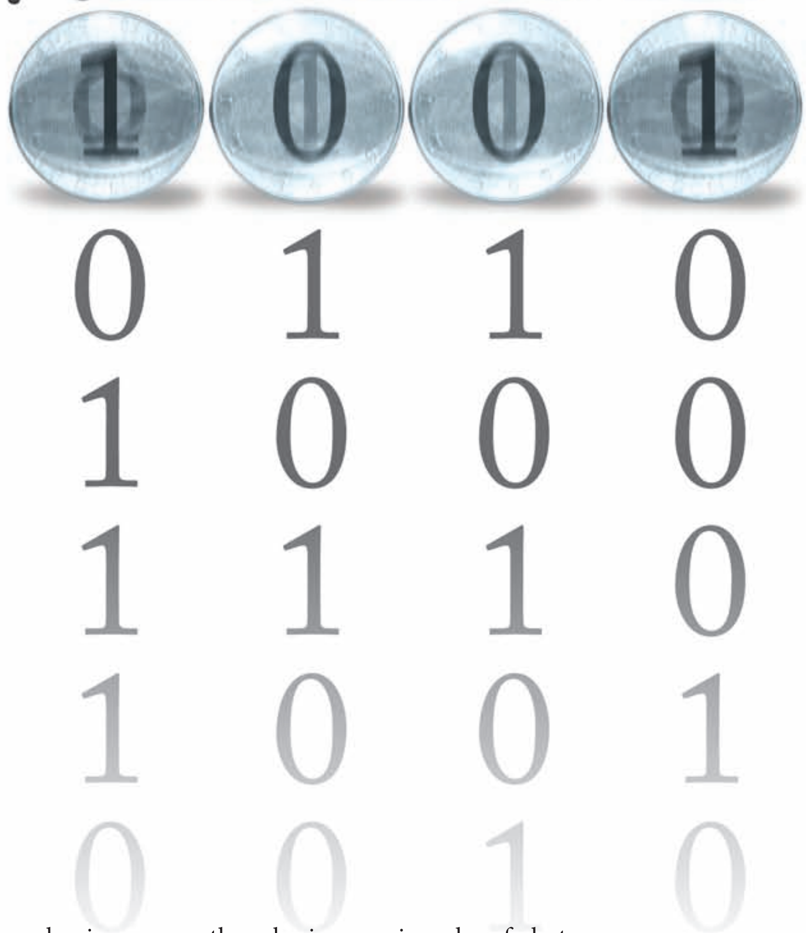
Quantum DISCORD

A distinguishing trait of quantum correlations discovered at Los Alamos may be the key to a quantum leap in computing technology.



Quantum mechanics governs the submicroscopic realm of photons, electrons, and atoms. In principle, its equations are valid for an object of any size, but a large object (and large, in this context, could mean anything bigger than 10 or 20 atoms) cannot effectively be isolated from its environment because it undergoes incessant interactions with the matter and radiation surrounding it. A process called decoherence ensues: information describing the object's complex quantum state disperses into the environment, forcing the object into simpler states without the quantum features of its pre-decoherence state. Thus, even as the combined whole—object plus environment—adheres to the quantum rules of behavior, the object alone no longer exhibits any of the telltale signatures of quantumness and, in effect, "goes classical."

The border territory between quantum and classical is becoming increasingly important for applications, and Los Alamos National Laboratory Fellow Wojciech Zurek is making inroads into this regime. Zurek has dedicated much of his career to an elusive line of research into the foundations of quantum physics. How does the quantum behavior of the microscopic world give way to the classical behavior of the macroscopic world? Why do electrons behave differently than baseballs? Just where does that transition lie, and what rules emerge from it? What aspects of the world are irreducibly quantum?

Most of Zurek's work is foundational in nature, but just like the advent of quantum theory itself, which long preceded its many practical applications, his pure research now appears capable of sparking a revolution in technology. By characterizing the degree of quantumness inherent in a system of particles, he may have also provided a foundational element in the budding field of quantum computing, from which tremendous computational power can be unleashed if the quantum states of many particles can be mixed in such a way as to allow a large number of simultaneous calculations.

Such simultaneity has its roots in the fact that a quantum system can exist in a quantum combination of states known as a superposition. A simple example is the spin orientation of a single electron. As with any such "spin-½ system," an electron has two possible quantum states referred to as "up" and "down" with respect to any chosen axis. When the spin of an electron is measured, the result is always up or down and is never in between. But prior to that measurement, the electron can exist in a superposition of both states, and it is this superposition that gives rise to the possibility of quantum computation. The idea is to replace a classical bit of information, with a value of either 0 or 1, with a quantum bit, or qubit, in a superposition of both 0 and 1. Because each qubit simultaneously involves both 0 and 1, N qubits can simultaneously represent 2^N distinct possibilities. This quantum parallelism, if harnessed, could make certain types of computations much faster, accomplishing feats impossible for the fastest existing computers.

To appreciate the distinction between a quantum and classical computer, consider each performing a simulation of a quantum system consisting solely of spin-½ states. The powerful (but classical) Roadrunner supercomputer at Los Alamos has enough memory to store the state of a system containing at most 43 quantum spins, because 2^{43} (that's 8.8 trillion) complex numbers are needed to accomplish this. Simulating a complete quantum state of a system with one more spin—a collection of 44 electrons, say—would require doubling Roadrunner's size. Yet, in principle, a quantum computer consisting of just 44 qubits could do the same job.

The trick to practical quantum computation is to get many qubits to work together while being careful not to disturb them, because a disturbance would ruin their superposition the same way a spin measurement causes an electron spin to settle on a particular state—up or down and not both. But if avoiding a disturbance means perfectly isolating the qubits from the environment to prevent decoherence (decoherence which would, at best, turn the quantum computer into a poorly performing classical computer), then actually building a quantum computer would be nearly impossible.

The Entangled Web We Weave

Before the quantum computing community absorbed Zurek's foundational work, they assumed that getting qubits to work together to exploit quantum parallelism required "entangling" them. Entanglement occurs when two or more particles interact with one another and then remain correlated long after the interaction is over. For example, physicists can entangle two electrons so that they have opposite spins, while maintaining their superposition: once measured, one electron's spin will be up and the other will be down, but which one is which can only be settled by measuring one of them. Prior to that measurement, each electron has, in a sense, both spins. Thus, two entangled particles can share a correlated superposition of states. This is what quantum computers need: qubits to hold multiple values simultaneously (through superposition) and operate in coordination with other qubits (through entanglement).

Unfortunately, it has so far proven impractical to maintain entangled superpositions long enough to carry out any sizable quantum computation. Whenever any one qubit is disturbed (decohered by an air molecule, perhaps, or a stray photon of light), the entire entanglement collapses. And successful quantum computers capable of performing valuable tasks, such as detailed simulations for the development of advanced materials, would need to sustain thousands of entangled qubits such that none is disturbed.

The struggle to protect such a large-scale entanglement against an inescapable background of disturbances was

More than just answering a fundamental question— ***What makes a correlation quantum?****—quantum discord may provide the basis for significant technological progress.*

beginning to seem like a permanent deal-breaker until a proof-of-principle quantum computation was carried out using a less restrictive correlation among qubits than entanglement. That successful demonstration was based on Zurek's work.

When Mess is More

In 2000, Zurek proposed a new way to evaluate the quantumness of correlations between particles. He and Harold Ollivier, a graduate student who did part of his Ph.D. research with Zurek, used this new quantity to explore the effect of decoherence on quantum correlations. Zurek and Ollivier quantified the strength of the invisible quantum correlations by taking the quantum mutual information of a pair of qubits—a measure of how much the qubits "know" about each other—and subtracting from it the mutual information one would attribute to the pair if the correlation were classical. The result was dubbed discord. It quantifies the disagreement between the quantum and classical ways of calculating the same property.

Before discord, the sole criterion for the quantumness of correlation between particles was entanglement. All entangled states have discord. However, even when all entanglement has been eliminated by decoherence, Zurek and Ollivier showed, discord can still remain. Discord, then, measures how much of the correlation between particles is irreducibly quantum in nature. It is a more inclusive standard of correlation than entanglement, but because states that have substantial discord need not be entangled, it's also less sensitive to disturbances.

Zurek and Ollivier originally set out to explore the boundary between quantum and classical behavior using discord. The state of a pair of microscopic systems, such as entangled electrons with spins that are simultaneously up and down, is sharply changed by measurement and, therefore, the discord of an entangled electron pair is large. And a macroscopic object, such as a cup of coffee, is already decohered by the environment, so it doesn't observably change when something about it is measured; thus, its correlations with other objects have vanishing discord. But because the heart of a quantum computer lies in between these two extremes—it is "mesoscopic," perhaps, and very difficult to isolate from its environment to protect its entanglement—discord has helped restore the hope that such a computer can still be built.

Indeed, recent research has shown that quantum computing can be carried out without any entanglement, but in all such cases discord plays an important role. It is an open question whether quantum computing requires exactly the quantum correlation given by the formula for discord, but this question is now front and center, investigated in hundreds of scientific papers over the past few years. More than just answering a fundamental question—What makes a correlation quantum?—quantum discord may provide the basis for significant technological progress. A computer with qubits correlated by discord rather than entanglement requires less protection against external disturbances—and perhaps that difference will enable the first functioning prototype.

Now that discord has been shown to suffice for some types of quantum computation, researchers can focus on the question of why it suffices. Discord is a relatively new concept in quantum physics circles and has yet to be fully explored. Perhaps it will prove useful in many other contexts as well. Or maybe it's just a coincidence that it holds such practical value in this one. Regardless, Zurek hopes the recent focus on discord will lead to a deeper understanding of the quantum underpinnings of our world—and open the door to a quantum leap in technology. ❖ LDRD

—*Craig Tyler*